Task 3

CPA or chosen plaintext attack

The origins of this type of attack could potentially be hundreds of years old but probably the most famous instance in relatively modern history comes from World War 2, Allied forces often made movements just so that axis forces would send a communication about it which once intercepted, they would already know what the plain text is and they now have the cipher for it, meaning they could try to reverse engineer it. Similar thing is true today, Google uses encryption for all of its search traffic which usually includes ads as well. This means that an attacker could by paying google get it to encrypt a plaintext of their choosing as well. This kind of attack is known as chosen plaintext attack.

An encryption scheme is secure against chosen plaintext attack if for every polynomial time adversary, adversary wins with probability of at most 0.5 + negl(n) in the game defined below:

1. The key k is chosen at random in {0,1} ^n and fixed.
2. Adversary gets the length of the key 1 ^n as input.
3. Adversary interacts with E for $t = poly(n)$ rounds as follows: in the i^{th} round, Adversary chooses a message m_i and obtains $c_i = E_k(m_i)$.
4. Then Adversary chooses two messages m_0, m_1, and gets $c^* = E_k(m_b)$ for $b \leftarrow_R \{0, 1\}$.
5. Adversary wins if it outputs b.

Now, with the introduction of step 3 which wasn't there in the earlier encryption scheme we have seen so far, we need to have a strictly stronger scheme.

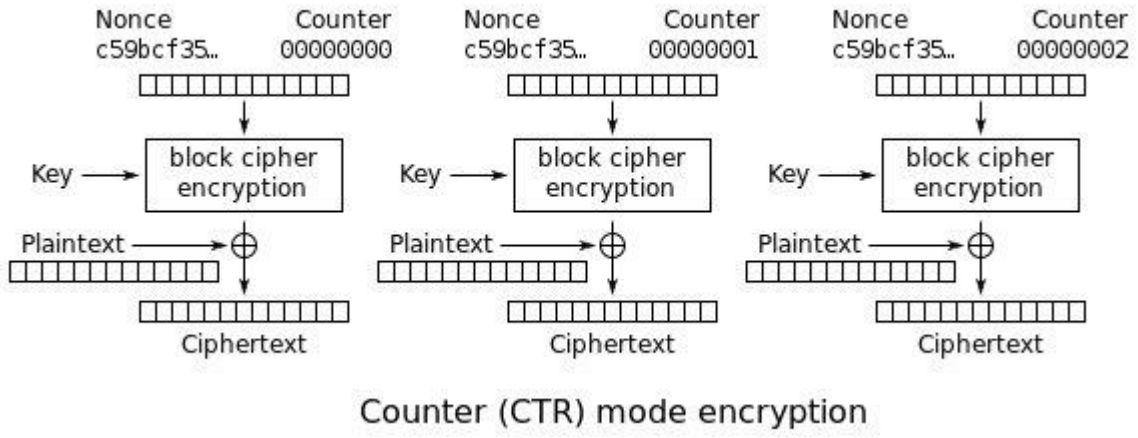
Build Algorithm

Theorem: There is no CPA secure encryption scheme (E, D) where E is deterministic.

The idea here becomes that we instead use a probabilistic encryption scheme.

Idea : c = (r, F(k) xor m), where r is a randomly generated number, F(k) is a secure encryption scheme and m is the message.

In this case, I have used randomized counter mode as the mode of operation for encryption.



Counter (CTR) mode encryption

Here, Counter is the initialization Vector taken as input or can be a randomly chosen number. The plaintext to be encrypted is divided into blocks of equal sizes as that of Counter. Counter is passed to prf with Key, k and the encrypted text is xor with the message block which forms a cipher text 1, counter is then incremented and process is repeated for each message block.

Proof

Theorem: If F is a pseudorandom function, then randomized counter mode has indistinguishable encryptions under a chosen plaintext attack.

We first prove that randomized counter mode is CPA-secure when a truly random function is used, and then since, we have already seen that for our PRF, the numbers generated are indistinguishable from the truly randomly generated number for polynomial time adversary, we can infer that it works with PRF as well.

Let ctr* denote the initial value ctr, when the challenge ciphertext is generated in the experiment Priv .

For the i block of the message, thus ctr*+i was used to generate f(ctr*+i).

Now, if ctr*+i was never accessed before, then the key stream is random and like a one time pad. Thus, the adversary has no advantage in deciding whether m0 or m1 was the corresponding plaintext for the challenge ciphertext.

So, we must find what is the probability that ctr*+i was actually "matches" with one of the queries of the adversary A

The adversary A makes q(n) queries. The starting IV value for the ith query is denoted by ctr. Let each message be of block-length, q(n).

We divide the entire scenario into two mutually exclusive cases:

1) There do not exist any i, j, j' for which ctr*+j=ctr '.
2) There exists i,j,j' for which ctr*+j=ctr +j'.

   In this case, A can easily determine f(ctr*+j) = f(ctr +j') and thus compute mj. Thus he can

predict whether m0 or m1 was encrypted.

Let Overlap denote the even that the sequence ctr +1,...,ctr +q(n) overlaps the sequence ctr*+1,...,ctr*+q(n).

Consider, ctr*+1,...,ctr*+q(n)

Overlap occurs when, ctr + 1 <= ctr*+q(n) and

when ctr + q(n) >= ctr*+1

This happens when: ctr*+1- q(n) <= ctr <= ctr*+q(n)-1

We define the event Overlap, as when Overlap_i occurs for any i,

$$\text{that is: } \Pr[\text{Overlap}] \le \sum \Pr[\text{Overlap}_i]$$

Now, $\Pr[\text{Overlap}_i] = 2q(n) - 1/2 \text{ ^n} \Rightarrow \Pr[\text{Overlap}] \le \frac{2q(n)^2}{2^n}$

$$\Pr[\text{Pr iv}^{\text{CPA}} = 1] \le \Pr[Overlap] + \Pr[\text{Pr iv}^{\text{CPA}} = 1 | Overlap]$$

$\Pr[\text{Pr iv}^{\text{CPA}} = 1]$ <= 2q(n) ^2/2 ^n + ½

Therefore, since the probability is <= 2q(n) ^2/2 ^n + ½, we infer that the randomized counter mode of operation is cpa secure.